Doxing trends and challenges - position statement

Doxing is the intentional online exposure of an individual's identity, private information or personal details without their consent.

Sharing the information publicly undermines the target's privacy, security, safety and/or reputation. Often those responsible for doxing urge others to use the information to harass the person targeted.

Background

Revealing private information about a person without their consent is not new. However, the increased use of internet connected technologies has made it far easier to collect, store, track and then share the information very publicly. The growth of online platforms has also expanded the network of people able to harass, humiliate or attack someone once their identifying details have been revealed.

Doxing is an abbreviation for 'dropping documents'. The information that is doxed may be sourced through publicly available information, research of public records or through unauthorised access to private databases and computer systems (hacking).

Unlike defamation, doxing does not have to reveal something untrue or damaging about an individual — the information is usually accurate, whether or not it has been sourced lawfully.

'Doxing' can refer to a number of different practices, including:

- deanonymizing doxing — revealing the identity of someone who was previously anonymous (for example, someone who uses a pseudonym)
- targeting doxing — revealing specific information about someone that allows them to be contacted or located, or their online security to be breached (for example, their phone number or home address, or their account username and password)
- delegitimizing doxing — revealing sensitive or intimate information about someone that can damage their credibility or reputation (for example, their private medical, legal, or financial records, or personal messages and photos usually kept out of public view).

Research points to a variety of motivations for doxing. In some cases, doxing is motivated by wanting to expose wrongdoing and hold the wrongdoer to account. It can also be used to exert control over someone following a relationship breakdown.

The threat of doxing can also be used to intimidate or threaten someone. In some cases, it is used to extort money, but often no demands are made to stop the information being released and the target is not even aware they are about to be doxed.

Anyone can be doxed and, regardless of the motive, the exposure of personal information violates the target's privacy and can compromise their safety. Reports of doxing made to eSafety indicate that it can lead to serious emotional, psychological and physical harms.

Doxing can leave the target vulnerable to, and fearful of:

- public embarrassment, humiliation or shaming
- discrimination, if personal characteristics are disclosed
- cyberstalking and physical stalking
- identity theft and financial fraud
- damage to their personal and professional reputation, leading to social and financial disadvantage
- increased anxiety
- reduced confidence and self-esteem.

The harms can be immediate, but they can also be ongoing if the information continues to be shared or stored by others.

On a broader level, using doxing as a form of digital vigilantism can have a negative impact on society through increasing lawlessness, conflict and reducing trust in public figures.

Recent coverage

In recent years there have been a number of high-profile examples of doxing.

In 'GamerGate' in 2014 a group of male gamers doxed female developers accusing them of politicising the industry. The Ashley Madison dox in 2015 exposed the details of the adult website's users.

During the COVID-19 pandemic, thousands of email addresses and passwords from employees of the World Health Organization, Gates Foundation and other institutions involved in the public health response have been posted on the internet, as well as those who have suffered from the virus.

There is debate over whether doxing can be considered a legitimate tool in public interest journalism, for example when the revelation of private information exposes contradictory, unethical or illegal behaviour. Doxing has been used in internet vigilantism against criminal activity such as online scams.

There is only limited research into the prevalence of doxing.

eSafety approach

eSafety has a multi-pronged approach to doxing:

- We are working to raise awareness about doxing, through position statements like these and with relevant partner organisations, so Australians are informed about the issue and the steps they can take if they experience doxing.
- We support Australian children who are victims of doxing, through our legislated cyberbullying reporting scheme and we help adults who are targeted, as part of our informal adult cyber abuse scheme.
- We work with social media services on serious cases, to have content removed using our existing relationships and escalation pathways.
- We support industry through our Safety by Design initiative, guiding them on the development and implementation of policies and systems for preventing and responding to doxing on their platforms.
- We refer victims to law enforcement agencies where there are immediate risks of violence or serious physical harm.

Advice for dealing with doxing

How to help protect yourself against doxing

- Check privacy settings on social media accounts, ensuring that you know who can see the content you share and who has access to your personal information.
- Use a range of strong passwords for your accounts, and ensure that any security questions are sufficiently difficult to guess.
- Try to set unique usernames for each online account you use.
- Use secure authentication on all accounts, including two-factor authentication where available.
- Limit the amount of personal information that you share online, such as your address, place of work or study, or personal phone numbers.
- Make a habit of searching for yourself online in incognito mode, to see how much of your information is accessible to others.

What to do if you are doxed

- Collect and preserve evidence of the doxing.
- Report to the social media platform where the doxed material is posted — The eSafety Guide provides the relevant links for many popular platforms and services.
- Block unwanted contact — The eSafety Guide also provides many of these links.
- Seek further support or assistance from the police, eSafety or a legal, counselling or support service.
- Review and update your privacy and security settings.

If you are at risk of immediate harm, call Triple Zero (000).

For more information, read eSafety's advice on responding to adult cyber abuse.

Published: 29 May 2020